Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Tesina de Grado

Facultad de Informática

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Motivación

- Cantidad de sistemas informáticos en continuo crecimiento.
- Gestión de usuarios convertida en un problema relevante.
- Mismos usuarios acceden a diferentes aplicaciones.
- Necesidad de usuario/clave único.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Motivación

- Desarrollos en plataformas diferentes y sistemas operativos heterogéneos.
- Desarrolladores de aplicaciones deben implementar el manejo de identidades en cada aplicación.
- Necesidad de independizar la gestión de usuarios de los sistemas.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Motivación

- Los usuarios no pueden dar o delegar permisos a otros usuarios según su criterio.
- Control central de derechos de acceso.
- Área de administración de la seguridad es la responsable de las políticas.
- Necesidad de tener conocimientos técnicos específicos.
- Administrar los derechos de acceso de manera amigable.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo
Autenticación única

- Proceso de autenticación sesión/usuario.
- El usuario provee sus credenciales una sola vez.
- Accede a todas las aplicaciones permitidas.
- Usuarios no autenticados son derivados al servicio de autenticación.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo
Autenticación única

- Beneficios:
  - Política de autenticación /autorización uniforme.
  - Desarrolladores no necesitan implementar el módulo de autenticación / autorización.
  - Reducción de pedidos de recuperación de contraseñas.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Control de acceso basado en roles

Objetivo

- El usuario final no es el dueño de la información a la cual se le permite acceder.
- El dueño de la información es la organización misma.
- Decisiones de control de acceso:
  - Funciones.
  - Responsabilidades.
  - Tareas.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo

Control de acceso basado en roles

- RoI: Transacciones que puede realizar.
- Transacción: Acceso a las funciones e información.
- Miembros gestionados por el personal de seguridad informática.
- Proteger la integridad de la información
- Quién puede realizar que acción sobre que información.
- Puede utilizarse para políticas de separación de funciones.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo

Repositorio de usuarios

- Consolidación de la información de los usuarios.
- Repositorio centralizado.
- Alta, baja o modificación de cuentas y contraseñas de usuarios.
- Directorio.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo
Front-end de administración de usuarios / roles

- Independizar el control de acceso del área de desarrollo.
- Administrar derechos de acceso de manera amigable.
- Sin necesidad de tener conocimientos técnicos específicos.
- Aplicación web que permita la administración de usuarios y roles.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Objetivo
Front-end de administración de usuarios / roles

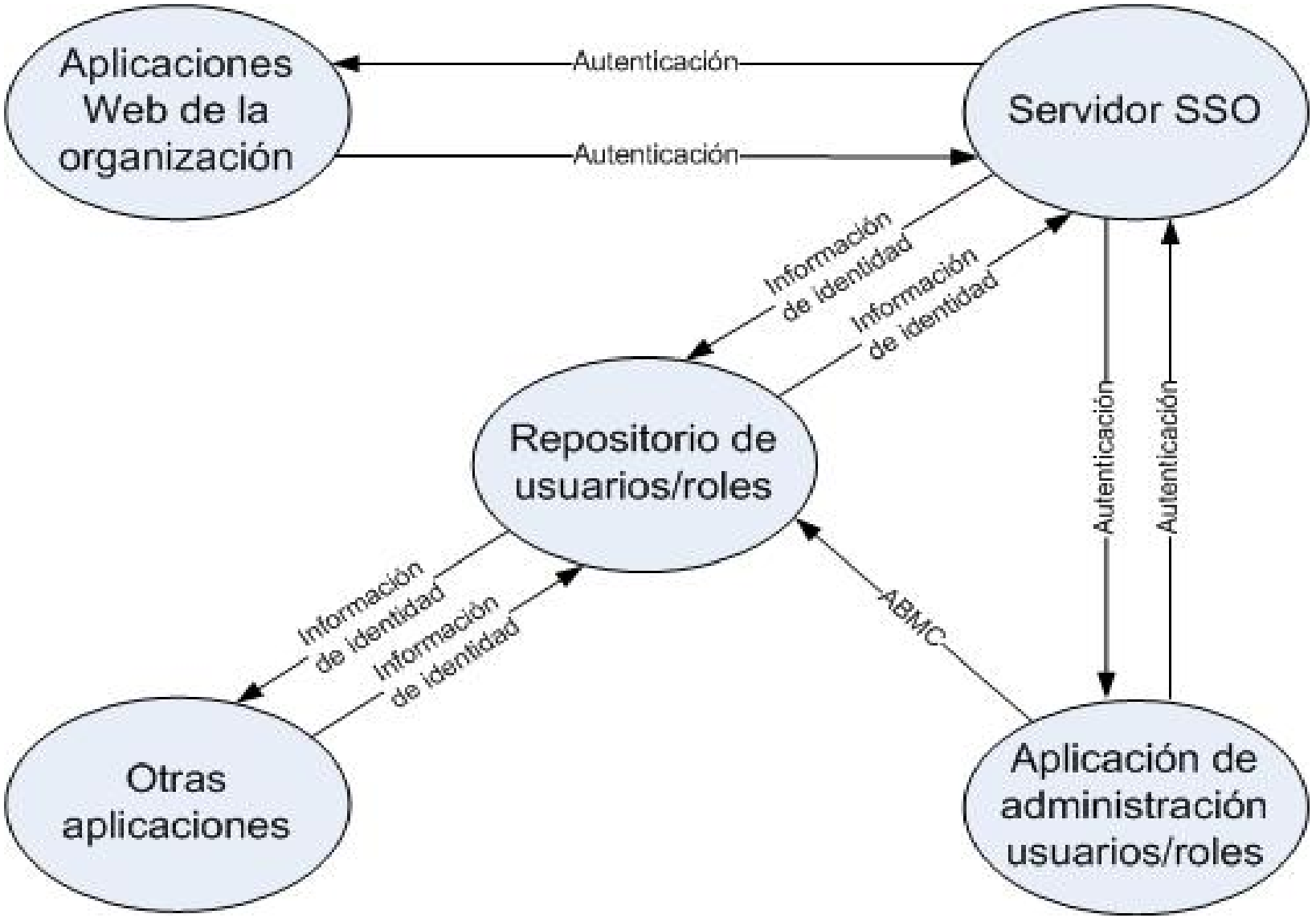
- Garantizar que se concedan o revoquen los derechos correctos.
- Simplificar la asignación de usuarios a roles.
- Cambiar las funciones de los usuarios durante su desempeño en la organización.
- Realizar estas actividades de forma correcta y de manera oportuna.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

- La aplicación deberá permitir:
  - Administrar aplicaciones
  - Administrar roles
  - Administrar usuarios
  - Administrar la asignación de roles a usuarios.

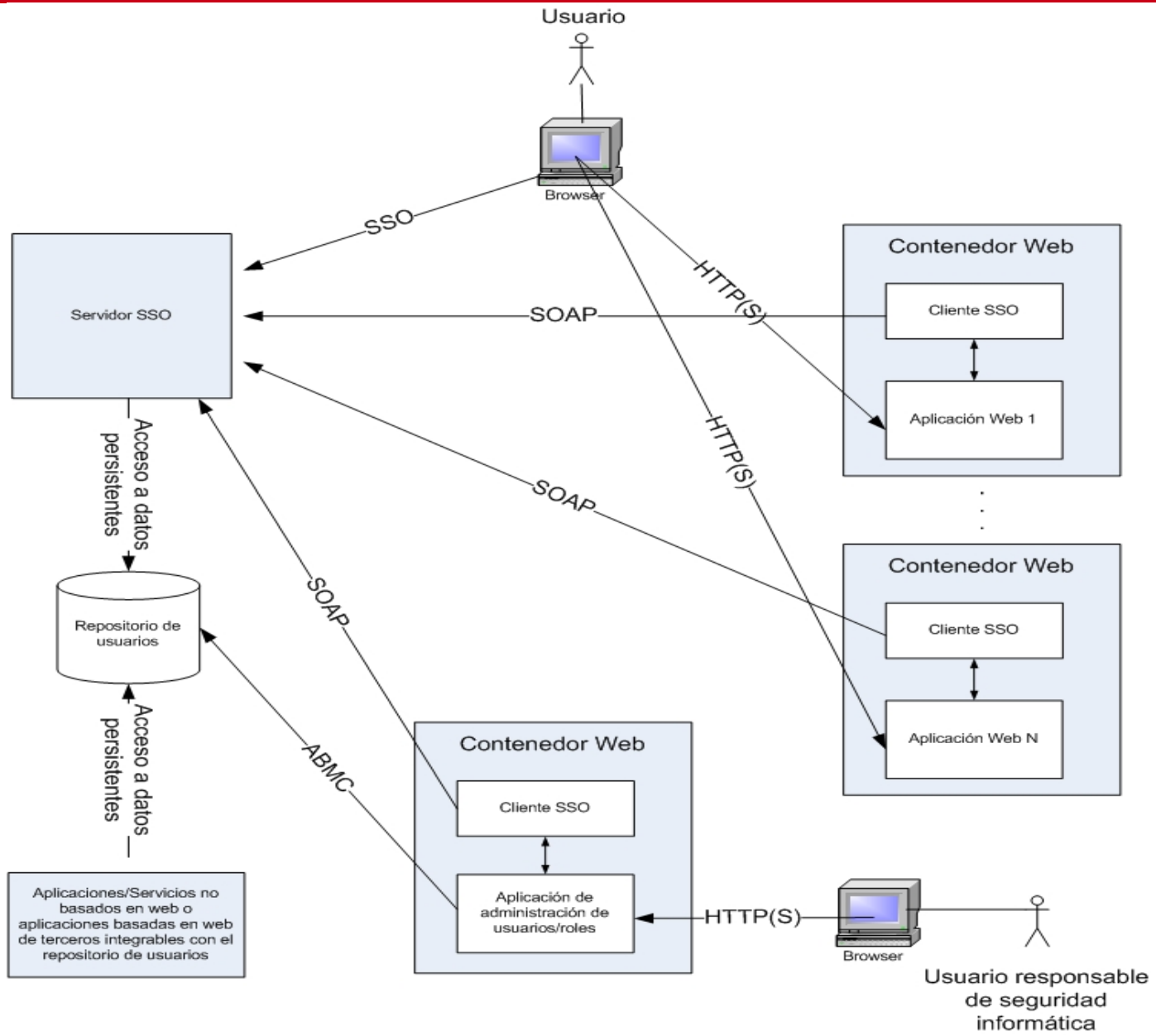
Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Interacción de componentes



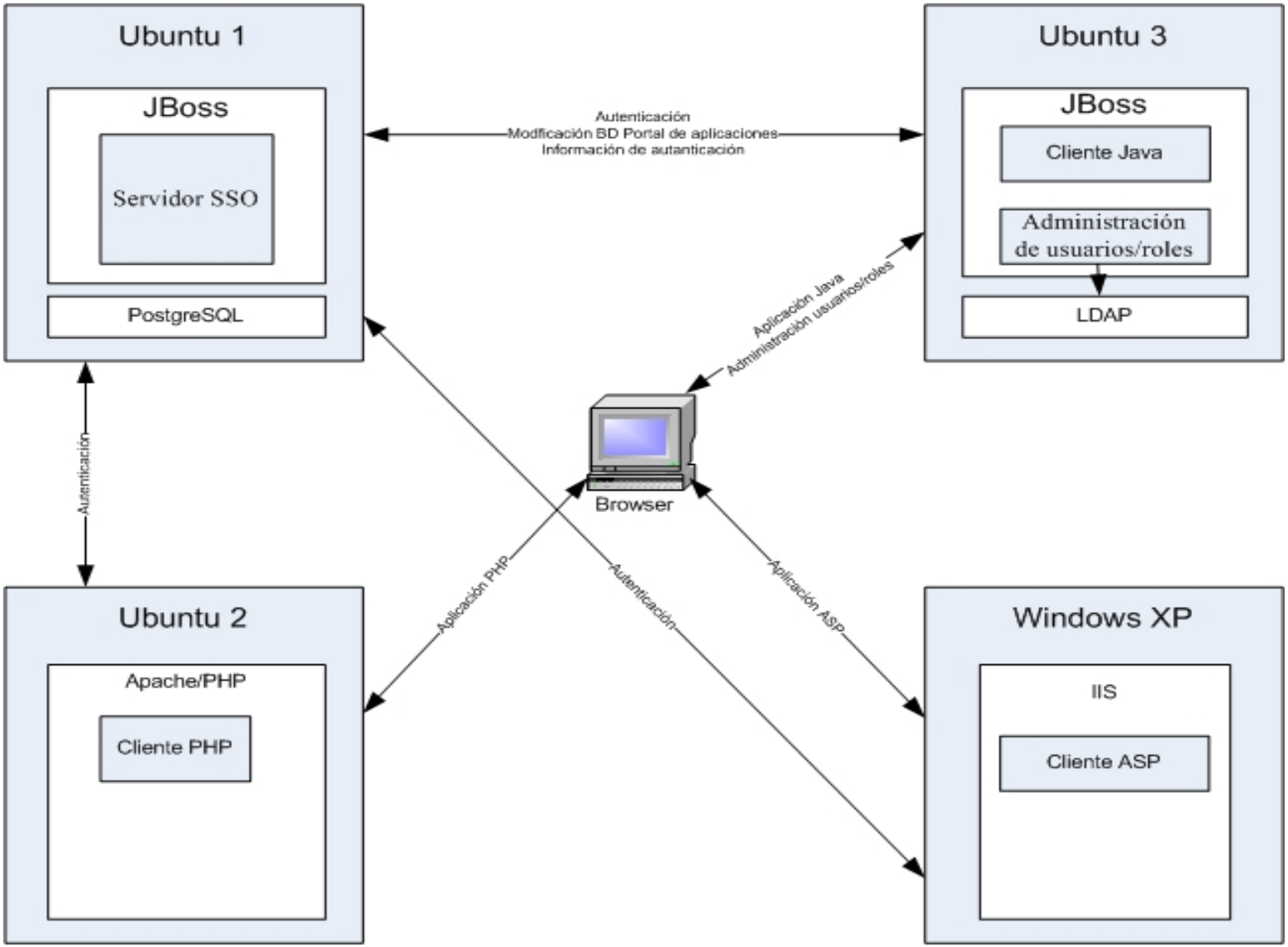
Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Arquitectura



Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Infraestructura



Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Conclusión

- Arquitectura para que las aplicaciones web desarrolladas en diferentes plataformas tengan la capacidad de SSO.
- Control de acceso basado en roles.
- Se desarrolló una aplicación de aprovisionamiento roles/usuarios.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

- La aplicación permite:
  - Independizar la seguridad informática del área de desarrollo.
  - Delegar responsabilidad a la oficina de seguridad informática.
  - Personal sin conocimientos técnicos específicos pueda realizar la actividad.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Conclusión

- Servicio de directorio permite:
  - Integrar un gran rango de aplicaciones externas
  - Interfaz de integración.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Conclusión

- Autenticación única en aplicaciones web desarrolladas dentro de la organización.
- Contraseña única para aplicaciones web de terceros o aplicaciones no web de la organización con soporte para LDAP.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

- Extensión:
  - Integración con la base de datos de RRHH.
  - Directorio virtual.
    - No hay necesidad de adaptación.
    - Visualizar cualquier base de datos como un servicio de directorios.

Una arquitectura y framework para que las aplicaciones manejen Single Sign-On

Muchas gracias